

Configuración de la conectividad vWAN del ISP dual de Azure en Secure Firewall

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Diagrama](#)

[Enlaces de acceso directo a Internet \(DIA\) duales \(Azure + FTD Load-Balancing/Redundancy\)](#)

[Configurar](#)

[Fase 1: Configuración del sitio VPN de Azure vWAN](#)

[Paso 1: Crear sitio VPN de Azure vWAN \(dispositivo FTD remoto\)](#)

[Paso 2: Configurar parámetros de Azure APIPA Gateway](#)

[Paso 3: Configurar parámetros VPN de sitio de Azure vWAN](#)

[Paso 4: Activar y activar APIPA BGP personalizado en instancias de enlace a sitios VPN](#)

[Paso 5: Descargar archivo de configuración del sitio VPN](#)

[Fase 2: Configuración de FTD para conectividad ISP dual a Azure vWAN](#)

[Paso 1: Análisis de la configuración VPN descargada](#)

[Paso 2: Configuración de Link BGP Update Source Loopback Interfaces](#)

[Paso 3: Configuración de objetos de política de fase 1/fase 2](#)

[Paso 4: Configuración de interfaces de túnel virtual \(VTI\)](#)

[Paso 5: Aprovisionamiento de topologías VPN IPsec](#)

[Paso 6: Validar topologías VPN](#)

[Paso 7: Configuración de ECMP](#)

[Paso 8: Configuración de BGP](#)

[Paso 9: Configuración de Trayectoria Múltiple eBGP](#)

[Verificar/Solucionar problemas](#)

Introducción

Este documento describe cómo configurar la conectividad VPN de sitio a sitio de Microsoft Azure Virtual WAN (vWAN) para Secure Firewall mediante enlaces WAN duales.

Prerequisites

Requirements

Cisco recomienda conocer estos temas:

- WAN virtual de Microsoft Azure (vWAN)
- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defence (FTD)

Asegúrese de que estos componentes se configuraron inicialmente en el entorno de Azure:

- Instancia de Microsoft Azure vWAN
- Hub vWAN de Microsoft Azure

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Secure FTD versión 10.0
- Cisco Secure FMC Versión 10.0
- Microsoft Azure vWAN

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Cuando el FTD de la sucursal tiene dos interfaces externas orientadas al proveedor de servicios de Internet (ISP), cada una puede conectarse de forma redundante y activa a Azure vWAN, por lo que se utiliza cada enlace ISP. Azure vWAN crea dos túneles IPsec por enlace de sitio, uno a Azure Hub Instance0 y otro a Instance1, de modo que cada interfaz ISP termina dos túneles. En ambos links ISP, esto da como resultado cuatro túneles IPsec que terminan en el FTD.

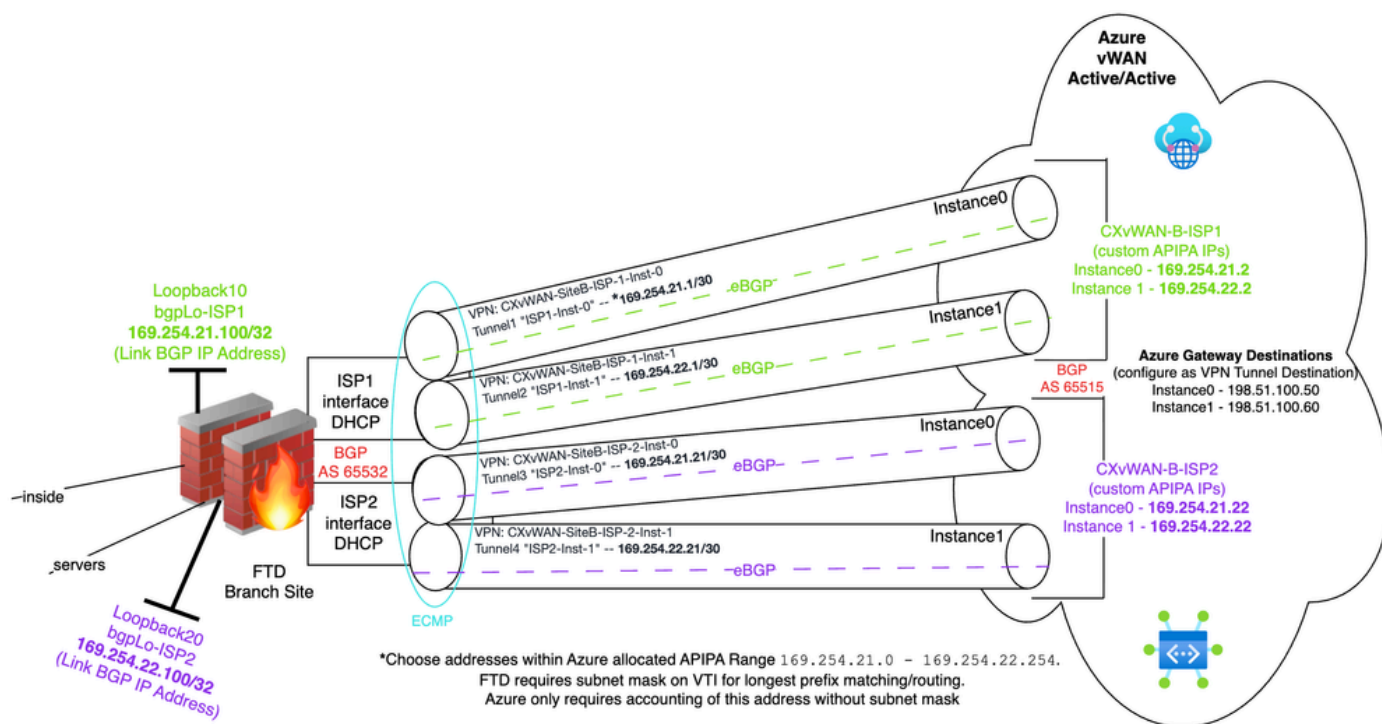
Las instancias de Azure funcionan en modo Activo/Activo para el equilibrio de carga y la redundancia, por lo que el FTD lo refleja a través de la configuración de múltiples rutas de igual costo (ECMP) en los cuatro túneles IPsec. Mediante el uso de direcciones IP privadas automáticas (APIPA) personalizadas, se establecen vecindades de protocolo de gateway fronterizo externo (eBGP) con números de sistema autónomo privado (ASN) distintos en cada uno

de los cuatro túneles. Esto habilita la funcionalidad de múltiples rutas BGP, proporcionando múltiples rutas redundantes a cada par de instancias de link de sitio de Azure Hub.

Diagrama

El diagrama muestra la topología de la configuración descrita en este artículo. La variante de enlace de acceso directo a Internet (DIA) dual origina ambos túneles de Azure desde dos interfaces externas en el FTD.

Enlaces de acceso directo a Internet (DIA) duales (Azure + FTD Load-Balancing/Redundancy)



Topología de conectividad de acceso directo a Internet dual

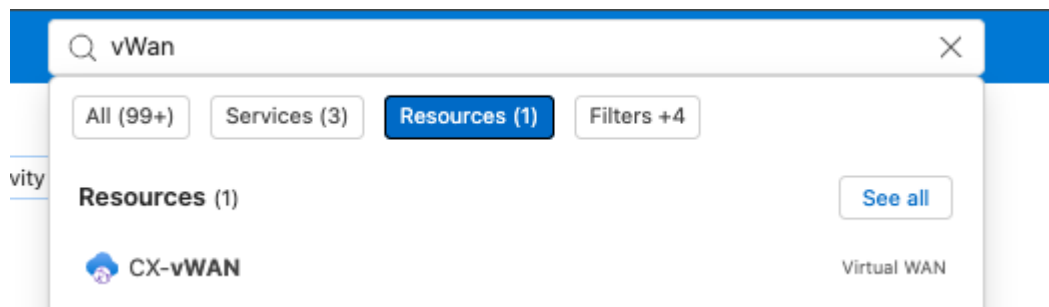
Configurar

Fase 1: Configuración del sitio VPN de Azure vWAN

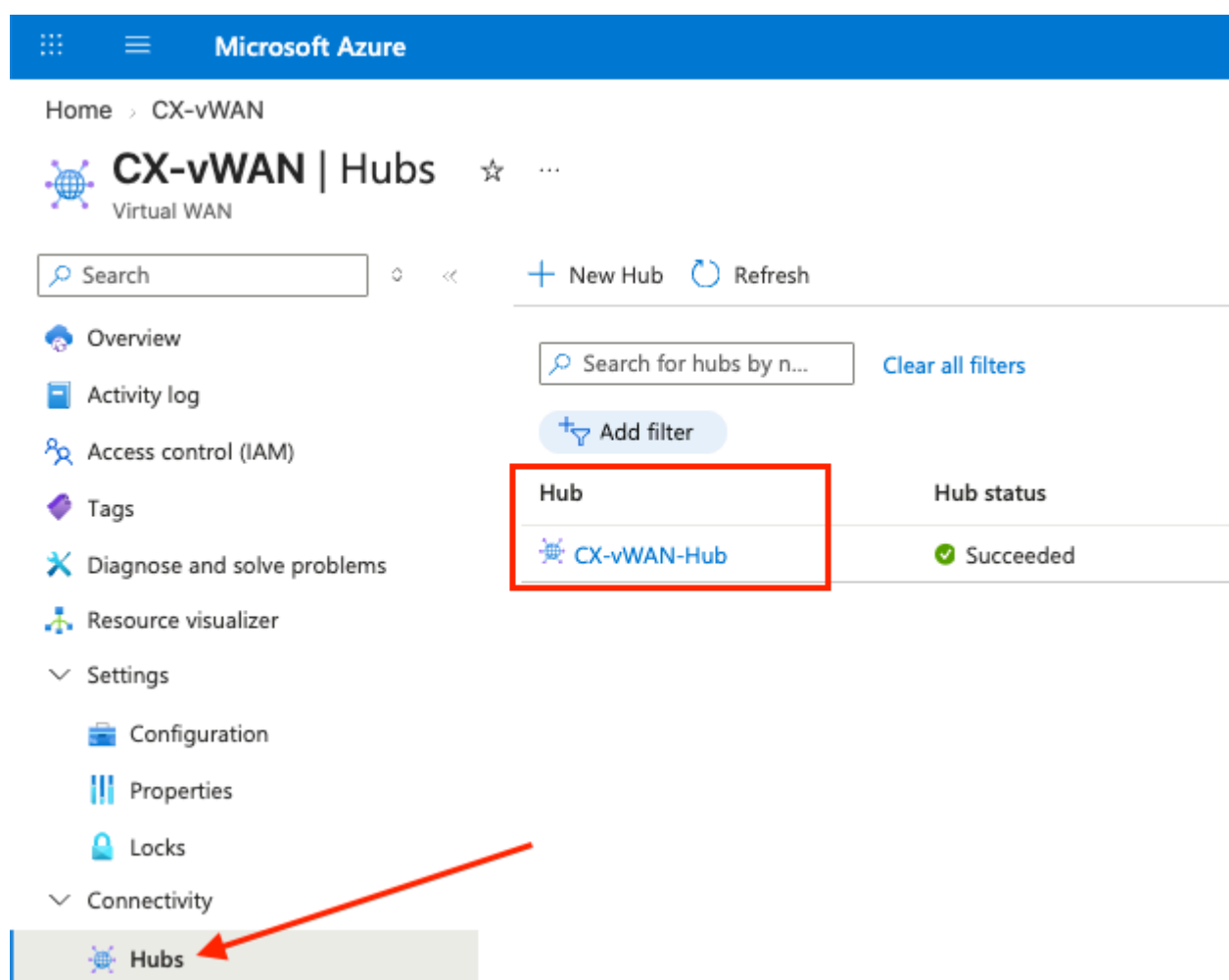
Paso 1: Crear sitio VPN de Azure vWAN (dispositivo FTD remoto)

1) Busque vWAN en el campo de búsqueda de Azure, haga clic en WAN virtuales para entrar en

el Azure vWAN Hub existente. A continuación, navegue hasta Conectividad > Concentradores y haga clic en el Azure vWAN Hub existente.



Búsqueda de consultas para WAN virtual



Seleccionar hub WAN virtual existente

2) Haga clic en Conectividad > VPN (de sitio a sitio) y haga clic en + Crear nuevo sitio VPN

Microsoft Azure

Home > CX-vWAN | Hubs > CX-vWAN-Hub

CX-vWAN-Hub | VPN (Site to site)

Virtual HUB

Search

Download VPN Config Packet Capture Delete gateway Reset gateway Monitor Gateway

Overview

Connectivity

VPN (Site to site)

ExpressRoute

User VPN (Point to site)

Routing

Security

Third party providers

Monitor

Essentials

Gateway configuration

NAT Rules

VPN Sites Metrics

Search this page Clear all filters

Hub association : **Connected** Add filter

VPN Sites

Check active filters when searching for a VPN site. VPN connectivity status might take a few minutes to refresh.

Create new VPN site Connect VPN sites Disconnect VPN sites Refresh

Page: 1

Site name	Location	Cloud
No results		

Crear nuevo sitio WAN virtual



Nota: El espacio en blanco que cubre los valores de varios campos de las imágenes es intencional para la publicación de este documento.

3) Introduzca los valores en los campos obligatorios. Cuando haya terminado, haga clic en Siguiente: Enlaces > para avanzar.

Create VPN site ...

Basics Links Review + create

Project details

Subscription

Resource group *

Instance details

Region *

Name *

Device vendor *

Private address space

At least one address space is required if BGP isn't configured. To configure BGP, please go to Links tab.

 You can also work with a Virtual WAN partner to create multiple sites simultaneously. [Learn more.](#)

Previous

Next : Links >

Parámetros generales de configuración del sitio VPN

4) Introduzca la información de enlace necesaria. La dirección BGP de enlace y el ASN de enlace son la dirección de destino de la capa 3 de BGP del túnel interno y el número de AS de BGP en el lado de la rama con el que se forma la vecindad en los túneles de sitio a sitio. La dirección BGP de vínculo es una dirección de subred no superpuesta (/32) fuera de la subred del espacio de direcciones privadas del concentrador configurado, que Azure instala como ruta /32 para alcanzar como vecino BGP. En las secciones posteriores del FTD se crean dos interfaces de loopback para representar la dirección BGP de enlace para cada uno de los links de sitio dual. La dirección IP de vínculo/nombre de dominio completo (FQDN) es la dirección IP de destino de capa 3 del encabezado externo del tráfico que va al sitio de la sucursal necesario para proporcionar conectividad de seguridad IP (IPsec)/Intercambio de claves de Internet versión 2 (IKEv2). Continúe con el paso siguiente cuando haya terminado haciendo clic en Siguiente : Revisar + crear >.



Nota: Asegúrese de revisar la documentación específica de Azure si usa direcciones que

van desde 169.254.21.0 a 169.254.22.255 para direcciones de túnel: [Elección de direcciones APIPA BGP.](#)

Create VPN site ...

Basics **Links** Review + create

Link Details ⓘ

Link name	Link speed	Link provider name	Link IP address / FQDN	Link BGP address	Link ASN	
ISP-1-Link	1000	ISP1		169.254.21.100	65532	...
ISP-2-Link	1000	ISP2		169.254.22.100	65532	...

i You can also work with a Virtual WAN partner to create multiple sites simultaneously. [Learn more.](#)

Previous

Next : Review + create >

Configurar parámetros de vínculo a sitios

5) Una vez confirmada la información, haga clic en Create (Crear).

Create VPN site ...

 Validation passed

- basics
- links
- Review + create**

The hub will be created under the same subscription and resource group as the vWAN.

Basics

Region	East US
Name	Dual-ISP-Site
Device vendor	Cisco
Private address space	
Links	

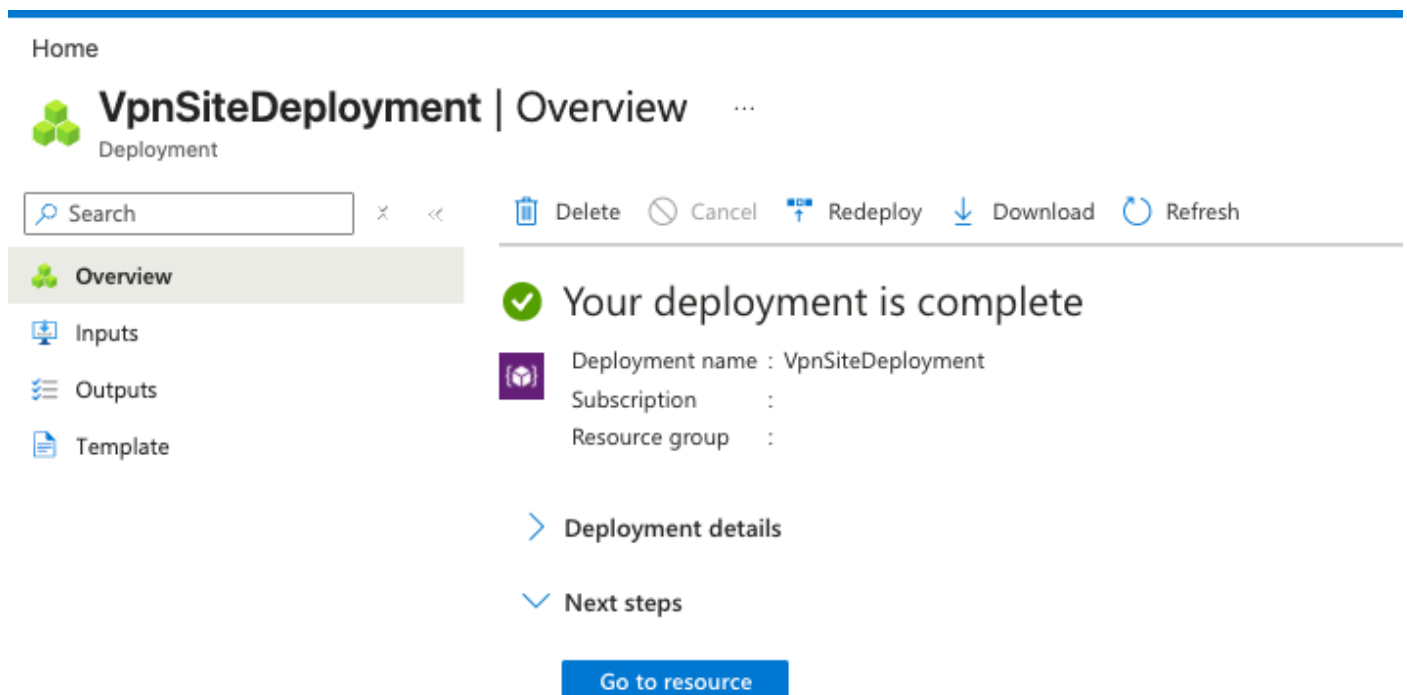
Link name	ISP-1-Link
Link provider name	ISP1
Link speed	1000
Link IP address / FQDN	
Link ASN	65532
Link BGP address	169.254.21.100

Link name	ISP-2-Link
Link provider name	ISP2
Link speed	1000
Link IP address / FQDN	
Link ASN	65532
Link BGP address	169.254.22.100

 You can also work with a Virtual WAN partner to create multiple sites simultaneously. [Learn more.](#)

Revisar y crear un nuevo sitio VPN

6) Una vez finalizada la implementación del sitio VPN, vuelva a la configuración del hub vWAN.



Home

VpnSiteDeployment | Overview

Deployment

Search

Delete Cancel Redeploy Download Refresh

Overview

- Inputs
- Outputs
- Template

✓ Your deployment is complete

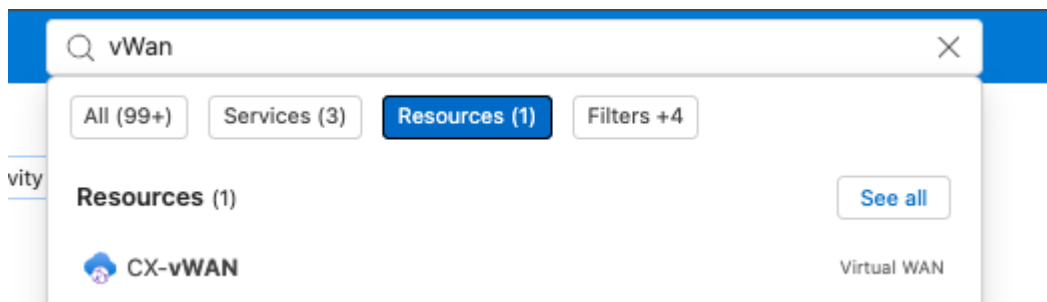
Deployment name : VpnSiteDeployment
Subscription :
Resource group :

> Deployment details

✓ Next steps

[Go to resource](#)

Progreso de implementación de sitio WAN virtual



Search vWan

All (99+) Services (3) **Resources (1)** Filters +4

Resources (1) [See all](#)

CX-vWAN Virtual WAN

Búsqueda de consultas para WAN virtual

Paso 2: Configurar parámetros de Azure APIPA Gateway

Azure requiere configuración adicional para las direcciones de Direcciones IP privadas automáticas (APIPA) en el espacio de direcciones IPv4 169.254.0.0/16.

1) Introduzca el hub existente mediante Connectivity > Hubs.

Microsoft Azure

Home > CX-vWAN

CX-vWAN | Hubs

Virtual WAN

Search

+ New Hub Refresh

Search for hubs by n... Clear all filters

Add filter

Hub	Hub status
CX-vWAN-Hub	Succeeded

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

- Configuration
- Properties
- Locks

Connectivity

Hubs

Vaya A Conectividad De Hub WAN Virtual

2) Vaya de nuevo a Conectividad > VPN (de sitio a sitio) y haga clic en el hipervínculo Configuración de la puerta de enlace.

CX-vWAN-Hub | VPN (Site to site)

Virtual HUB

Search

Download VPN Config Packet Capture Delete gateway Rese

Overview

Connectivity

VPN (Site to site)

ExpressRoute

User VPN (Point to site)

Routing

Connection Policies

Route Maps

Essentials

Gateway configuration : [1 scale unit - 500 Mbps x 2 \(View/Configure\)](#)

NAT Rules : [0 NAT Rule\(s\) \(Edit\)](#)

VPN Sites Metrics

Search this page Clear all filters

Hub association : **Connected** Add filter

VPN Sites ⓘ

Hipervínculo de configuración de gateway de acceso

3) Aparece un panel lateral para Editar Gateway VPN. Bajo Instancia0 de Gateway VPN e Instancia1 de Gateway VPN, ingrese dos direcciones IP BGP personalizadas únicas que actúan como IPs vecinas a cada instancia para vecindades BGP sobre los túneles IPsec. Esto es necesario si elige utilizar el direccionamiento APIPA dentro de esta topología. En el campo Peer Address, ingrese la IP de vecino BGP que se utilizará para alcanzar las instancias de Azure desde el FTD. Azure no intenta establecer BGP con el FTD si el direccionamiento APIPA está en uso, por lo tanto, el FTD intenta establecer el vecino eBGP en cada túnel con Azure.

El total sale a 2 links x 2 túneles implícitos; un túnel a Instance0 e Instance1 por link ISP; el total llega a cuatro túneles IPsec con vecindades BGP entre Azure y las dos interfaces FTD ISP.

Estas direcciones deben ser únicas y, en esta demostración, la segunda y última dirección de host de las subredes /30 asignadas a cada túnel debe configurarse en el FTD para su uso. Una vez configurado, haga clic en Editar.



Nota: Asegúrese de revisar la documentación específica de Azure si usa direcciones que van desde 169.254.21.0 a 169.254.22.255 para direcciones de túnel: [Elección de direcciones APIPA BGP](#)

Edit VPN Gateway



A Site to site (VPN gateway) enables you to connect VPN sites to a hub.

AS Number ⓘ

65515



Gateway scale units * ⓘ

1 scale unit - 500 Mbps x 2



Routing preference ⓘ

☒ Microsoft network ☐ Internet

VPN Gateway Instance 0

Public IP Address ⓘ

Private IP Address ⓘ

10.2.0.4

Default BGP IP Address ⓘ

10.2.0.12

Custom BGP IP Address ⓘ

169.254.21.22



169.254.21.2



Peer Address

VPN Gateway Instance 1

Public IP Address ⓘ

Private IP Address ⓘ

10.2.0.5

Default BGP IP Address ⓘ

10.2.0.13

Custom BGP IP Address ⓘ

169.254.22.22



169.254.22.2



Peer Address



Updating a hub can take 30 minutes or more. [Learn more.](#)

Edit

Cancel

Editar direcciones IP BGP personalizadas de gateway VPN



Nota: Como señala Azure, es posible que esto tarde hasta 30 minutos o más en actualizarse.

Paso 3: Configurar parámetros VPN de sitio de Azure vWAN

1) En la página Conectividad > VPN (sitio a sitio) dentro de la configuración del Azure vWAN Hub, y haga clic en la X para borrar la Asociación del Hub: Filtrado conectado para ver los sitios VPN desconectados.

The screenshot shows the Microsoft Azure portal interface for configuring a vWAN Hub. The breadcrumb trail is: Home > CX-vWAN | Hubs > CX-vWAN-Hub. The page title is 'CX-vWAN-Hub | VPN (Site to site)'. The left sidebar has a search bar and a navigation menu with 'Overview', 'Connectivity' (highlighted), 'ExpressRoute', 'User VPN (Point to site)', 'Routing', 'Security', 'Third party providers', and 'Monitor'. The 'Connectivity' section is expanded, showing 'VPN (Site to site)' as the selected option. The main area has a top bar with actions: 'Download VPN Config', 'Packet Capture', 'Delete gateway', 'Reset gateway', and 'Monitor Gateway'. Below this is the 'Essentials' section with 'Gateway configuration' and 'NAT Rules'. The 'VPN Sites' tab is active, showing a search bar and a filter bar. The filter bar contains 'Hub association : Connected' with a red 'X' icon next to it, and a red arrow points to this icon. There is also an 'Add filter' button. A message at the bottom states: 'Check active filters when searching for a VPN site. VPN connectivity status might take a few minutes to refresh.'

Borrar filtros de conexión de asociación de hub

2) Marque la casilla de verificación junto al sitio VPN provisionado recientemente y haga clic en Connect VPN Site.

 Download VPN Config  Packet Capture  Delete gateway  Reset gateway 

 Overview

▼ Connectivity

 **VPN (Site to site)**

 ExpressRoute

 User VPN (Point to site)

▼ Routing

 Connection Policies

 Route Maps

 Routing Intent and Routing Policies

 BGP Peers

 Route Tables

 Effective Routes

▼ Security

 Azure Firewall and Firewall Manager

▼ Third party providers

^ Essentials

Gateway configuration : [1 scale unit - 500 Mbps x 2 \(View/Configure\)](#)

NAT Rules : [0 NAT Rule\(s\) \(Edit\)](#)

VPN Sites Metrics

[Restore previous filters](#)

 Add filter

VPN Sites ⓘ



Check active filters when searching for a VPN site. VPN connectivity status might take a few mi

 Create new VPN site  **Connect VPN sites**  Disconnect VPN sites  Refresh

Page:

Site name

↑↓ Location

☒  **Dual-ISP-Site**

Acción del sitio de conexión VPN

3) Configure la clave precompartida (PSK) que desee y configure los parámetros IPsec deseados haciendo clic en la opción de alternancia Custom. Estos parámetros IPSec deben coincidir en la configuración de FMC/FTD en pasos posteriores. Para guardarlo, haga clic en Connect (Conectar).



Nota: La compatibilidad con Diffie-Hellman (DH) del grupo 24 se ha eliminado en la versión 6.7 del FTD/FMC.

Connect sites

Virtual HUB



Security settings

Pre-shared key (PSK) ⓘ

.....

Protocol

IKEv2

IKEv1

IPsec ⓘ

Default

Custom

i When using custom IPsec/IKE policies, please ensure that the custom settings are appropriately configured on the on-premise device for both initial tunnel establishment and rekey.

SA Lifetime in seconds * ⓘ

27000

IKE Phase 1 ⓘ

Encryption *

GCMAES256

Integrity/PRF *

SHA384

DH Group *

DHGroup14

IKE Phase 2(ipsec) ⓘ

IPsec Encryption *

GCMAES256

IPsec Integrity *

GCMAES256

PFS Group *

NONE

Propagate Default Route ⓘ

Enable

Disable

Use policy based traffic selector ⓘ

Enable

Disable

Configure traffic selector?

Yes

No

Connection Mode ⓘ

Default

Initiator Only

Responder Only

These sites will be connected to the [CX-vWAN-Hub] hub.

Site name	↑↓	Region	↑↓
 Dual-ISP-Site		eastus	

Connect

Configuración de la clave previamente compartida y los parámetros de IPsec

4) La confirmación del aprovisionamiento del sitio VPN se ha completado correctamente.

Notifications



[More events in the activity log →](#)

[Dismiss all](#)



Successfully created VPN connection



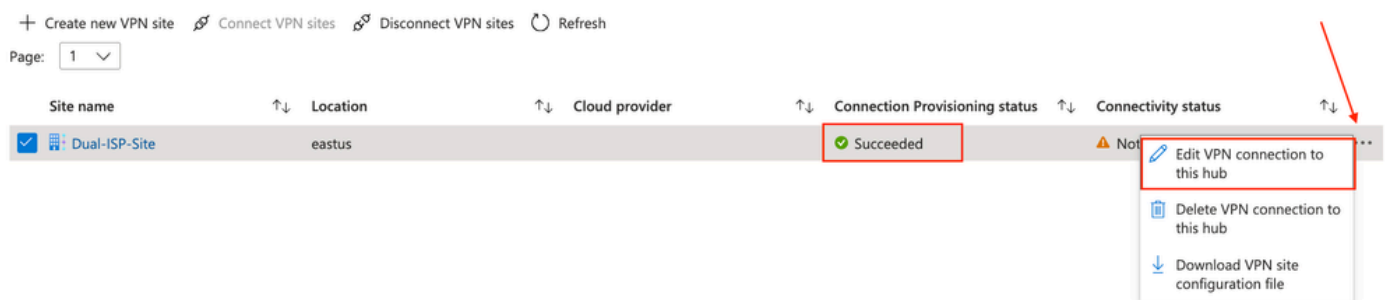
Successfully created VPN connection 'Connection-Dual-ISP-Site'.

a few seconds ago

Confirmar el estado de aprovisionamiento del sitio VPN

Paso 4: Activar y activar APIPA BGP personalizado en instancias de enlace a sitios VPN

1) Actualice la página VPN (de sitio a sitio) y confirme que la columna Estado de provisión de la conexión indica que la conexión se ha realizado correctamente, lo que le permite hacer clic en los puntos suspensivos y hacer clic en el elemento de menú desplegable Editar conexión VPN a este hub.



Validar la conexión correcta y editar la conexión VPN

2) Haga clic para configurar Link Connection 1 (ISP1) e ingrese la Pre-Shared Key (PSK) nuevamente, y asegúrese de hacer clic en el botón Enable junto a Custom BGP IP Address, y asigne cuál sería la dirección de host restante de las subredes /30 que serán los valores del campo de dirección IP de destino del túnel interno del encabezado IP BGP generado por los FTD.

Básicamente, el Túnel ISP1 VT11 a Azure Instance0 tiene una asignación de dirección de 169.254.21.1/30, y el segundo Túnel ISP1 VT12 que termina en el FTD tiene una IP de 169.254.22.1/30 asignada para la Instancia1.

Haga clic en Next (Siguiente): Link Connection 2> para continuar con los parámetros de enlace del ISP 2.



Nota: Es posible que necesite volver a ingresar su PSK y hacer clic nuevamente en la opción de grupo PFS alineado en el menú desplegable en Azure.

Edit VPN connection

Basics

Link connection 1

Link connection 2

Link name: ISP-1-Link

Link connection

Enable

Disable

Connection status: NotConnected

Pre-shared key (PSK) ⓘ

.....

Connection Mode ⓘ

Default

Initiator Only

Responder Only

Border gateway protocol ⓘ

Disable

Enable

Custom BGP IP Addresses ⓘ

Disable

Enable

Custom BGP IP Address

Instance 0 ⓘ

169.254.21.2

Instance 1 ⓘ

169.254.22.2

Use Azure Private IP Address ⓘ

Yes

No

Protocol

IKEv2

IKEv1

To change the protocol, please delete the connection first and then create a new connection.

Use policy based traffic selector ⓘ

Enable

Disable

IPsec ⓘ

Default

Custom

SA Lifetime in seconds * ⓘ

27000

IKE Phase 1 ⓘ

Encryption *

GCMAES256

Integrity/PRF *

SHA384

DH Group *

DHGroup14

IKE Phase 2(ipsec) ⓘ

IPsec Encryption *

GCMAES256

IPsec Integrity *

GCMAES256

PFS Group *

NONE

DPD timeout in seconds * ⓘ

45

Review + create

Previous

Next : Link connection 2 >

3) Repita los pasos anteriores y aplique los parámetros aplicables en Link Connection 2 (link ISP2). Al finalizar, haga clic en Create (Crear).

Edit VPN connection

Basics Link connection 1 Link connection 2

Link name: ISP-2-Link

Link connection Enable Disable

Connection status: NotConnected

Pre-shared key (PSK) ⓘ

Connection Mode ⓘ Default Initiator Only Responder Only

Border gateway protocol ⓘ Disable Enable

Custom BGP IP Addresses ⓘ Disable Enable

Custom BGP IP Address

Instance 0 ⓘ 169.254.21.22 ▼

Instance 1 ⓘ 169.254.22.22 ▼

Use Azure Private IP Address ⓘ Yes No

Protocol IKEv2 IKEv1

To change the protocol, please delete the connection first and then create a new connection.

Use policy based traffic selector ⓘ Enable Disable

IPsec ⓘ Default Custom

SA Lifetime in seconds * ⓘ 27000

IKE Phase 1 ⓘ

Encryption *	Integrity/PRF *	DH Group *
GCMAES256 ▼	SHA384 ▼	DHGroup14 ▼

IKE Phase 2(ipsec) ⓘ

IPsec Encryption *	IPsec Integrity *	PFS Group *
GCMAES256 ▼	GCMAES256 ▼	NONE ▼

DPD timeout in seconds * ⓘ 45

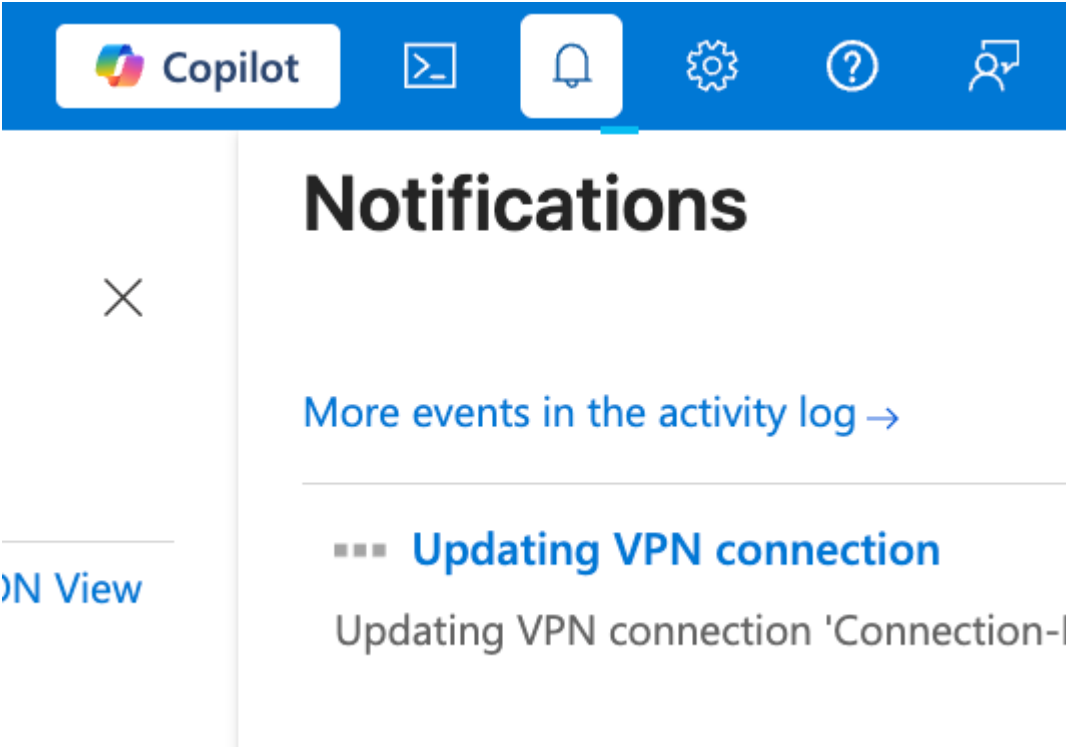
Create

Previous

Next

Configuración de la Conexión de Link Dos Configuraciones de BGP Personalizadas

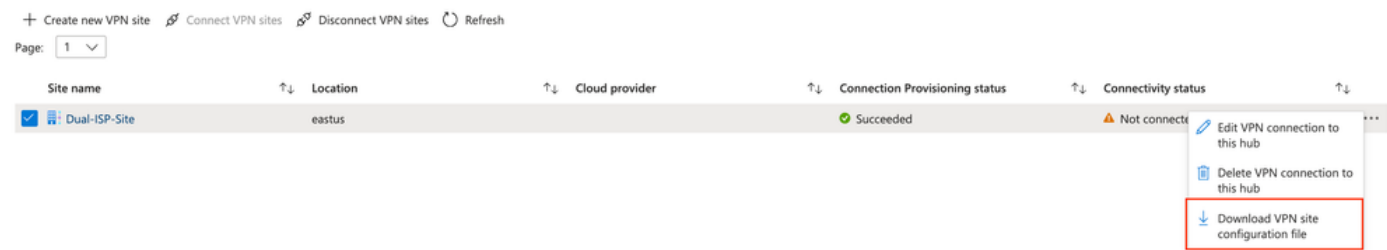
4) Las notificaciones de la interfaz de usuario de Azure muestran el inicio de la tarea de actualización.



Notificación de inicio de tarea de Azure Update

Paso 5: Descargar archivo de configuración del sitio VPN

1) En la misma página VPN (sitio a sitio) en Azure, elija el icono de puntos suspensivos en el extremo derecho del sitio VPN configurado y elija la opción Descargar archivo de configuración del sitio VPN.



Descargar opción de archivo de configuración de sitio VPN

2) Haga clic en el hipervínculo Click here to download.



Download Site-to-Site VP...



Dual-ISP-Site



Create new



Use existing



The file is ready to download



[Click here to download](#)



Descargar archivo de configuración del sitio VPN

Fase 2: Configuración de FTD para conectividad ISP dual a Azure vWAN

Paso 1: Análisis de la configuración VPN descargada

1) Abra el archivo de configuración descargado y aparecerá un resultado similar de JavaScript Object Notation (JSON). El resultado muestra uno de los dos objetos escritos en el archivo. Esta información proporciona un contexto útil para la configuración de FTD.



Nota: Para mejorar el enfoque, varios objetos irrelevantes y pares clave/valor se recortan para obtener brevedad.



Nota: Se invierte el orden de los objetos JSON ISP-Link-1 en el archivo descargado. Los puntos suspensivos del resultado del código representan el objeto ISP-2-Link con su configuración aplicable.

```
...
{
  "configurationVersion": {
    "LastUpdatedTime": "2026-09-25T20:20:26.7658453Z",
    "Version": "15221e61-4e2c-42f5-b9e4-96d674f5a9a3"
  },
  "vpnSiteConfiguration": {
    "Name": "Dual-ISP-Site",
    "IPAddress": "FTD_ISP1_WAN_IP",
```

```

    "BgpSetting": {
      "Asn": 65532,
      "BgpPeeringAddress": "169.254.21.100",
      "PeerWeight": 32768
    },
    "LinkName": "ISP-1-Link"
  },
  "vpnSiteConnections": [
    {
      "gatewayConfiguration": {
        "IpAddresses": {
          "Instance0": "Inst0IP",
          "Instance1": "Inst1IP"
        },
        "BgpSetting": {
          "Asn": 65515,
          "CustomBgpPeeringAddresses": {
            "Instance0": [
              "169.254.21.22",
              "169.254.21.2"
            ],
            "Instance1": [
              "169.254.22.22",
              "169.254.22.2"
            ]
          }
        }
      },
      "connectionConfiguration": {
        "IsBgpEnabled": true,
        "PSK": "PSK",
        "IPsecParameters": {
          "IpsecEncryption": "GCMAES256",
          "IpsecIntegrity": "GCMAES256",
          "IkeEncryption": "GCMAES256",
          "IkeIntegrity": "SHA384",
          "PfsGroup": "None",
          "DhGroup": "DHGroup14",
          "SALifeTimeInSeconds": 27000
        }
      }
    }
  ]
}
]

```

Mantenga este resultado como referencia a medida que complete los pasos.

Paso 2: Configuración de Link BGP Update Source Loopback Interfaces

Las entradas de configuración de vecino BGP en el proceso BGP de FTD (configuradas en pasos posteriores del FTD) necesitan un origen estable que represente la configuración de Link BGP IP Address en Azure Site Link correspondiente.

1) Vaya a Devices > Device Management.

Cloud-delivered Firewall Management Center
Devices / Device Management

Monitor

- Insights & Reports >
- Events & Logs >
- Insights & Reports >

Manage

- Policies >
- Objects
- Devices**

Devices

- Device Management** ✓
- Upgrade
- Template Management
- Threat Defense Upgrade
- Platform Settings
- Chassis Upgrade
- FlexConfig
- Certificates

— Show less

Vaya A Administración De Dispositivos En Firepower Management Center



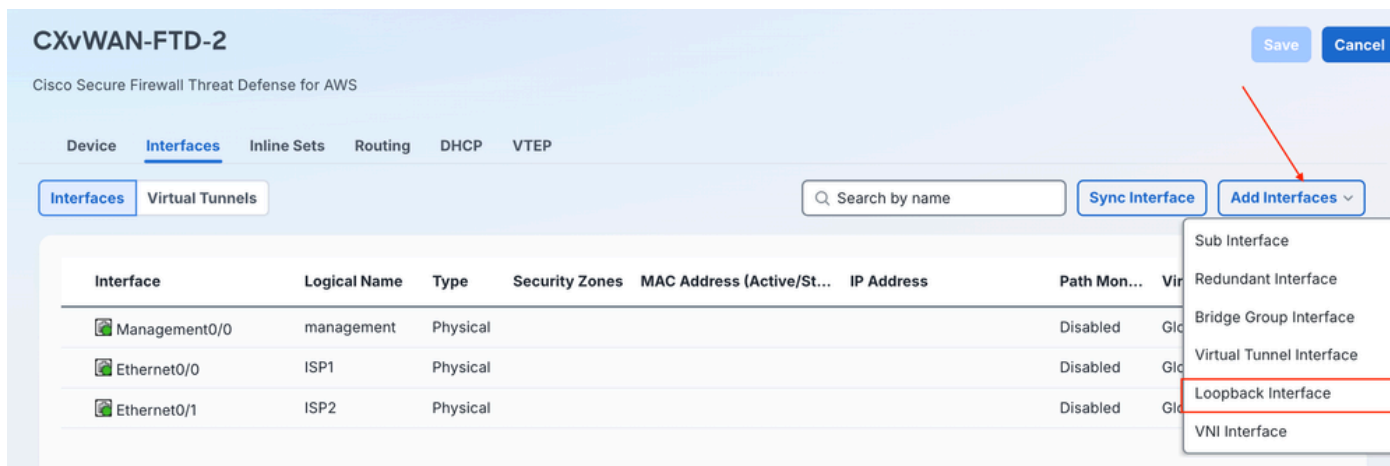
Nota: Este laboratorio utiliza el centro de gestión de firewall (cdFMC) proporcionado en la nube; sin embargo, los pasos siguen siendo los mismos para el FMC in situ.

2) Haga clic en el FTD que está configurando como dispositivo VPN de sucursal/sitio con conectividad ISP dual.

N/A - ROUTED	
☐	✓ CXvWAN-FTD-2 N/A - ROUTED
	10.0.0

Seleccione el FTD para la implementación de la configuración

3) Haga clic en el menú desplegable Add Interfaces y haga clic en Loopback Interface.



Agregar Interfaz De Loopback Al Dispositivo

4) Introduzca un Nombre de la interfaz de bucle invertido, asegúrese de activar la casilla de control Activado e introduzca un ID de bucle invertido. Introduzca una Descripción si lo desea. Una vez finalizado, haga clic en la pestaña IPv4.

Configuración De Información De Interfaz De Loopback Y Dirección IPv4

5) Ingrese la dirección IP de loopback para que sea la dirección IP de BGP de link configurada en pasos anteriores para el link del sitio ISP1 en Azure. Esta IP se utiliza como el origen de actualización BGP en las vecindades configuradas entre el FTD y las instancias de Azure sobre ISP1.



Nota: Puede hacer referencia al valor definido previamente en la configuración JSON de VPN descargada bajo `vpnSiteConfiguration.BgpSetting.BgpPeeringAddress` para ISP1

Add Loopback Interface ?

General **IPv4** IPv6

IP Type:

IP Address:

e.g. 192.168.1.1/255.255.255.0 or 192.168.1.1/24

[Cancel](#) [OK](#)

Introduzca La Dirección IPv4 Del Bucle Invertido Y Pulse Aceptar

6) Repita los subpasos c-e en esta secuencia para la configuración de loopback BGP ISP2.

Loopback10	bgpLo-ISP1	Loopb...	169.254.21.100/32(Static);	Disabled	Global	
Loopback20	bgpLo-ISP2	Loopb...	169.254.22.100/32(Static);	Disabled	Global	

Creación de Interfaces Loopback Primera y Segunda

7) Guarde su configuración.

You have unsaved changes [Save](#) [Cancel](#)

Guardar cambios

Paso 3: Configuración de objetos de política de fase 1/fase 2

1) Para configurar una configuración IKEv2/IPsec coincidente en el FMC con topologías VPN FTD, navegue hasta Manage > Objects, desplácese en el menú de navegación hasta VPN y expanda el submenú. Configure la política de fase 1 de IKEv2 seleccionando IKEv2 Policy en el menú y haciendo clic en Add IKEv2 Policy.

IKEv2 Policy

Internet Key Exchange (IKE) is a key management protocol that is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs). IKEv2 proposal, you can select multiple algorithms and modulus groups in one policy

[Add IKEv2 Policy](#)

Name		
AES-GCM-NUL-SHA		
AES-GCM-NUL-SHA-LATEST		
AES-SHA-SHA		
AES-SHA-SHA-LATEST		
DES-SHA-SHA		
DES-SHA-SHA-LATEST		
Umbrella-AES-GCM-256		

Displaying 1 - 7 of 7 rows | < < Page 1 of 1 >

Crear nuevo objeto de directiva IKEv2

2) Introduzca un nombre para la nueva política IKEv2, seleccione Prioridad y/o Duración. Asegúrese de que la política coincida en ambos extremos del túnel con respecto a la integridad, el cifrado, la función pseudoaleatoria (PRF) y el grupo DH. Elija los elementos Algorithm/Group que coincidirán con la configuración de Azure y haga clic en Add.



Nota: Puede hacer referencia a estos valores exactos dentro del archivo de configuración descargado en `vpnSiteConnections[0].connectionConfiguration.IPsecParameters`

New IKEv2 Policy

Name:*

Description:

Priority:* (1-65535)

Lifetime: seconds (120-2147483647)

Integrity Algorithms
Encryption Algorithms
PRF Algorithms
Diffie-Hellman Group

MD5
SHA
SHA512
SHA256
SHA384
NULL

Add

SHA256

Cancel Save

Crear política IKEv2

3) Una vez finalizada la configuración, haga clic en Guardar.

Edit IKEv2 Policy

Name:*

Description:

Priority:* (1-65535)

Lifetime: seconds (120-2147483647)

Integrity Algorithms
Encryption Algorithms
PRF Algorithms
Diffie-Hellman Group

1
2
5
14
15
16
19
20

Add

14

Cancel Save

Guardar la política IKEv2

4) Configure los parámetros de Fase 2/IPSec en el submenú Propuesta IPSec IKEv2 y haga clic en Agregar propuesta IPSec IKEv2.

IKEv2 IPsec Proposal

IPsec security association negotiation with ISAKMP, the peers agree to use a particular proposal to protect a particular data flow. In IKEv2 IPsec Proposal object, you can specify the encryption and authentication algorithms. Only the algorithms that are supported by both peers are allowed. During IKEv2 negotiations, the peers select the most appropriate options that each support.

Add IKEv2 IPsec Proposal

Name
AES-GCM
AES-SHA
DES_SHA-1
Umbrella-AES-GCM-256

Crear propuesta IKEv2 IPsec

5) Asigne un nombre a la propuesta IPsec de IKEv2 y asegúrese de que coinciden los mismos parámetros. Una vez hecho esto, haga clic en Guardar.

Edit IKEv2 IPsec Proposal



Name:*

Azure_IPsec

Description:

Available Algorithms

ESP Hash

ESP Encryption

AES-GCM-256

AES-256

AES-GCM-192

AES-192

AES-GCM

AES

3DES

DES

Add

Selected Algorithms

AES-GCM-256



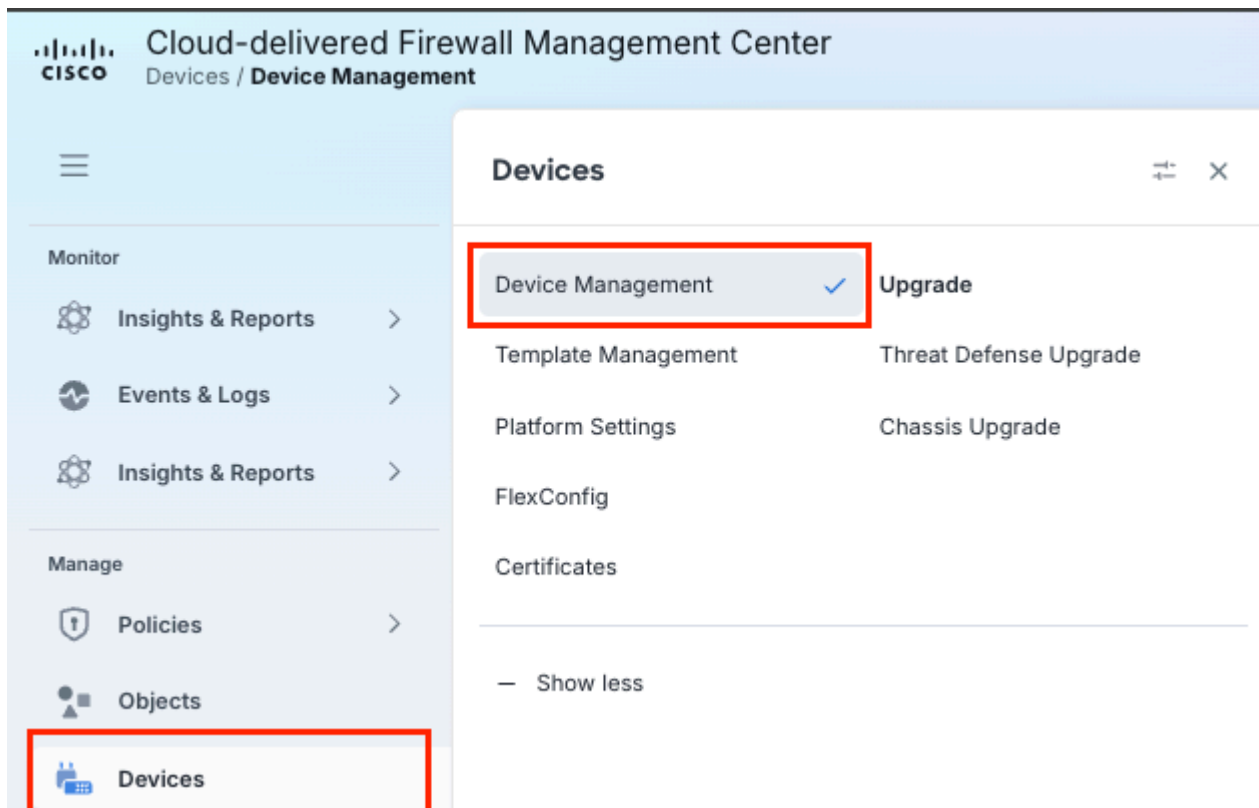
Cancel

Save

Nombre la propuesta IKEv2 IPsec y haga clic en Guardar

Paso 4: Configuración de interfaces de túnel virtual (VTI)

1) Vaya a Devices > Device Management.



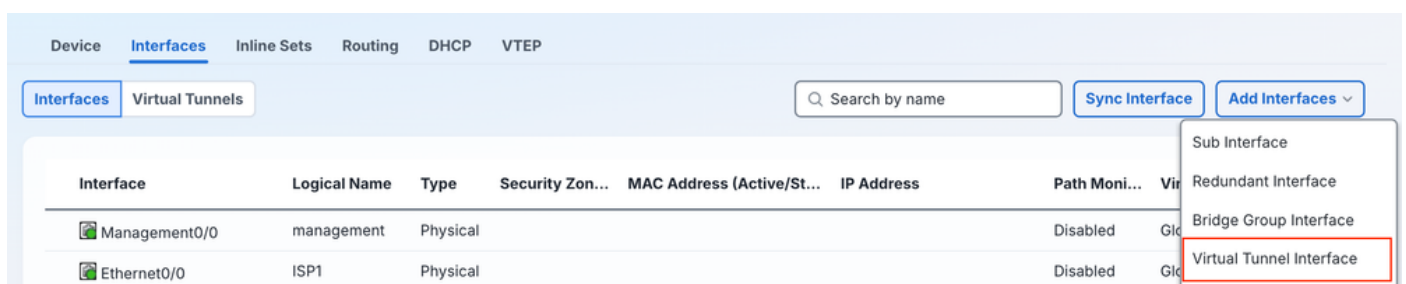
Vaya A Administración De Dispositivos En Firepower Management Center

2) Haga clic en el FTD que está configurando como dispositivo VPN de sucursal/sitio con conectividad ISP dual.

	✓ CXvWAN-FTD-2 N/A - ROUTED	10.0.0
---	---	--------

Seleccione el FTD para la implementación de la configuración

3) Haga clic en el menú desplegable Add Interfaces y elija Virtual Tunnel Interface (VTI).



Crear interfaz de túnel virtual

4) Introduzca la información del túnel. Asegúrese de que la casilla de verificación Enabled esté marcada, de que se ingrese Name (Description también, si se desea) y de que se elija Security Zone opcional. Alinee la interfaz ISP primaria correcta para configurar el VTI en y configure la dirección IP apropiada para la conectividad IPsec de túnel interno para el VTI. Pulse Aceptar cuando haya terminado.



Consejo: El diagrama de referencia muestra más contexto sobre la configuración potencial de VPN para la conectividad dual-WAN de Azure con FTD.

Add Virtual Tunnel Interface



Tunnel Type

☒ Static ☐ Dynamic

Name:*

ISP1-Inst-0

☒ Enabled

Description:

For "CXvWAN-SiteB-ISP-1-Inst-0" VPN topology

Security Zone:

Azure-Spoke-Zone

Priority:

0

(0 - 65535)

Propagate Security Group Tag: ☒

Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

Tunnel ID:*

1

(0 - 10413)

Tunnel Source:*

Ethernet0/0 (ISP1)

Dynamic

IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:*

☒ IPv4 ☐ IPv6

IP Address:*

☒ Configure IP

169.254.21.1/30



Cancel

OK

5) Configure 3 VTIs adicionales entre las interfaces ISP1 e ISP2 principales.

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router
Management0/0	management	Physical				Disabled	Global
Ethernet0/0	ISP1	Physical				Disabled	Global
Tunnel1	ISP1-Inst-0	VTI	Azure-Spoke-Zone		169.254.21.1/30(Static);	Disabled	Global
Tunnel2	ISP1-Inst-1	VTI	Azure-Spoke-Zone		169.254.22.1/30(Static);	Disabled	Global
Ethernet0/1	ISP2	Physical				Disabled	Global
Tunnel3	ISP2-Inst-0	VTI	Azure-Spoke-Zone		169.254.21.21/30(Static);	Disabled	Global
Tunnel4	ISP2-Inst-1	VTI	Azure-Spoke-Zone		169.254.22.21/30(Static);	Disabled	Global
Loopback10	bgpLo-ISP1	Loopback			169.254.21.100/32(Static);	Disabled	Global
Loopback20	bgpLo-ISP2	Loopback			169.254.22.100/32(Static);	Disabled	Global

Configuración de Interfaces de Túnel Virtual Adicionales

f) Asegúrese de hacer clic en Guardar para guardar los cambios.

You have unsaved changes

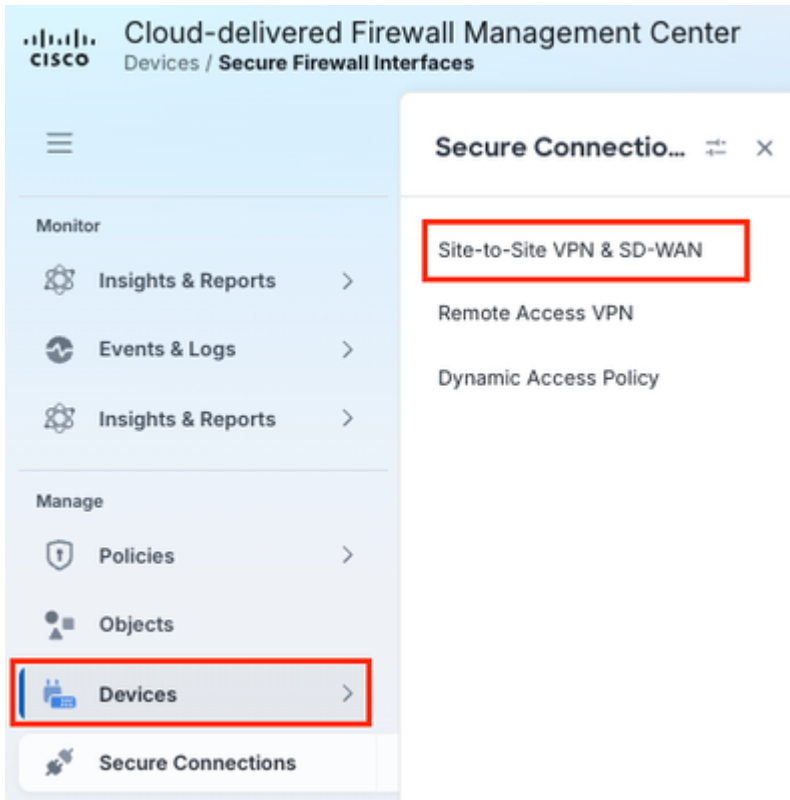
Save

Cancel

Guardar cambios

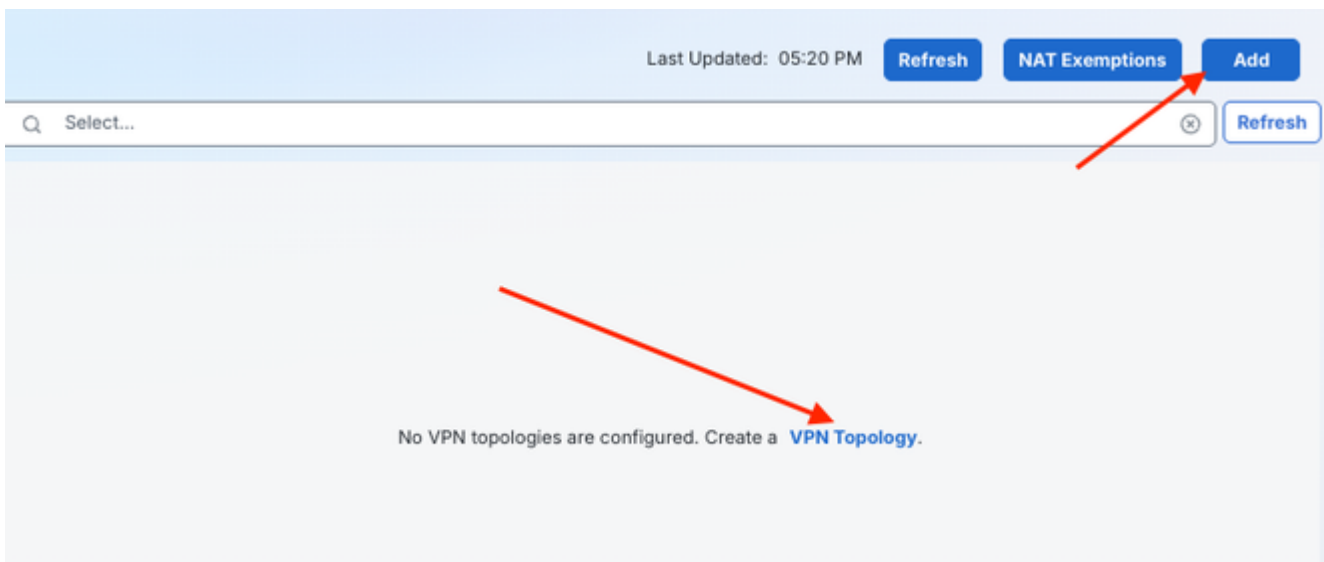
Paso 5: Aprovisionamiento de topologías VPN IPsec

1) Vaya a Administrar > Conexiones seguras > VPN de sitio a sitio y SD-WAN.



Gestionar las conexiones VPN y SD-WAN de sitio a sitio

2) Haga clic en el hipervínculo de configuración VPN Topology inicial en medio de la salida inicial, o haga clic en el botón Add.



Agregar nueva configuración de topología de VPN

3) Ingrese un nombre de topología para el primer túnel a través del link ISP1 a Azure Instance0. Haga clic en el botón de opción Route-Based VPN y haga clic en el tipo de topología Peer to Peer VPN. Una vez completado, haga clic en Create.

Create VPN Topology

Topology name *
CXvWAN-SiteB-ISP-1-Inst-0

VPN Type

SD-WAN Topology
Simplifies and automates the VPN and routing configuration in a hub and spoke topology, enabling SD-WAN capabilities.

Select VPN Topology

☐ Hub and Spoke

Prerequisites

Route-Based VPN
Secures traffic dynamically between peers based on routing over Virtual Tunnel Interfaces.

Select VPN Topology

☐ Hub and Spoke

☒ Peer to Peer

Policy-Based VPN
Secures traffic between peers based on a static policy using protected networks.

Select VPN Topology

☐ Hub and Spoke

☐ Peer to Peer

☐ Full Mesh

SASE Topology

⚠ SASE topology cannot be selected because Secure Access and Umbrella are not configured.

Prerequisites

Refresh

Cancel Create

Configuración del Tipo de Topología VPN Basada en Ruta

4) En primer lugar, elija el dispositivo Nodo A y en la lista desplegable Dispositivo que indica que el FTD termina los túneles VPN de Azure. Después de que el asistente obtenga las VTI disponibles del dispositivo, seleccione la VTI adecuada para la interfaz principal y la instancia que está configurando en el menú desplegable. En el menú Dispositivo del Nodo B, elija el lado de Azure para que sea el nodo Extranet en la configuración de topología VPN. Asegúrese de configurar un nombre descriptivo para el Nodo B, así como de introducir la Dirección IP del Extremo apropiada. Una vez completada, haga clic en la pestaña IKE para implementar la configuración de túnel de fase 1.



Nota: Puede hacer referencia a los valores de la dirección IP del terminal de la instancia en el archivo de configuración descargado en
`vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance0` y
`vpnSiteConnections[0].gatewayConfiguration.IpAddresses.Instance1`

Edit VPN Topology

Topology Name:*
CXvWAN-SiteB-ISP-1-Inst-0

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:
Point to Point Hub and Spoke Full Mesh

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints IKE IPsec Advanced

Node A

Device:*
CXvWAN-FTD-2

Virtual Tunnel Interface:*
ISP1-Inst-0 (IP: 169.254.21.1) +

Tunnel Source IP is Dynamic (DHCP) [Edit VTI](#)

Tunnel Source IP Address:*

☐ Send Local Identity to Peers

[+ Add Backup VTI \(optional\)](#)

Additional

Node B

Device:*
Extranet

Device Name*:
Azure-ISP1-Link-Inst0

Endpoint IP Address*:

[Cancel](#) [Save](#)

Definir Terminales De Topología De Nodo A Y Nodo B

5) Desplácese en el menú de navegación hasta Configuración de IKEv2 y haga clic en el icono del lápiz para editar las directivas según la directiva IKEv2 configurada recientemente. A continuación, elija la opción Pre-shared Manual Key en el menú desplegable Authentication Type e ingrese el PSK previamente configurado en Azure. Una vez completado, haga clic en la pestaña IPsec para configurar los parámetros de túnel IPsec de fase 2.



Nota: Puede hacer referencia a la clave previamente compartida en el archivo de configuración descargado en
`vpnSiteConnections[0].connectionConfiguration.IPsecParameters.PSK`

Edit VPN Topology

Topology Name:*
CXvWAN-SiteB-ISP-1-Inst-0

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:
Point to Point Hub and Spoke Full Mesh

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints **IKE** IPsec Advanced

IKEv2 Settings

Policies:* Azure_IKEv2 

Authentication Type: Pre-shared Manual Key

Key:*

Confirm Key:*

☐ Enforce hex-based pre-shared key only

Cancel Save

Editar configuración IKEv2 y clave de autenticación

6) Haga clic en el icono de lápiz adyacente al conjunto de transformación de propuestas IPsec para IKEv2, y elija los parámetros de política IPsec previamente configurados. Asegúrese de cambiar el valor Lifetime Duration para que coincida con la configuración VPN vWAN de Azure. Una vez confirmada la información configurada, haga clic en Guardar.



Nota: Puede hacer referencia al valor Lifetime en el archivo de configuración descargado en `vpnSiteConnections[0].connectionConfiguration.IPsecParameters.SALifeTimeInSeconds`

Edit VPN Topology

Topology Name:*

CXvWAN-SiteB-ISP-1-Inst-0

☐ Policy Based (Crypto Map) ☒ Route Based (VTI)

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:*

☐ IKEv1

☒ IKEv2

Endpoints

IKE

IPsec

Advanced

Transform Sets: IKEv1 IPsec Proposals IKEv2 IPsec Proposals*

tunnel_aes256_sha

Azure_IPsec

☐ Enable Security Association (SA) Strength Enforcement

☐ Enable Perfect Forward Secrecy

Modulus Group:



Lifetime Duration*:

27000

Seconds (Range 120-2147483647)

Lifetime Size:

Unlimited

Kbytes (Range 10-2147483647)

Cancel

Save

Configurar la duración de la propuesta IPsec

7) Repita los pasos secundarios anteriores en el paso 5 para crear los otros túneles de Azure a través de ISP1 Instance1, ISP2 Instance0 e ISP2 Instance1.

> CXvWAN-SiteB-ISP-1-Inst-0	Route Based (VTI)	Point-to-Point	Deployment Pending	✓		
> CXvWAN-SiteB-ISP-1-Inst-1	Route Based (VTI)	Point-to-Point	Deployment Pending	✓		
> CXvWAN-SiteB-ISP-2-Inst-0	Route Based (VTI)	Point-to-Point	Deployment Pending	✓		
> CXvWAN-SiteB-ISP-2-Inst-1	Route Based (VTI)	Point-to-Point	0- Tunnels	✓		

Crear topologías VPN sitio a sitio adicionales

Paso 6: Validar topologías VPN

Entre en system support diagnostic-cli, escriba en y presione enter (CLI de sólo lectura).

1) Compruebe la conectividad del túnel IKE de fase 1.

```
`show crypto isakmp sa | i UP|READY`
```

2) Compruebe la conectividad IPsec Phase 2.

```
show crypto ipsec sa | i int|current_peer|pkts
```



Nota: Cuando se visualizan los resultados de las asociaciones de seguridad (SA) IPsec y los contadores pkts decaps y pkts decrypt aumentan, pero los paquetes encaps y pkts encrypt no lo hacen, esto es lo que se espera en este escenario. Azure está intentando formar vecindades BGP a través de las direcciones del espacio de IP privada del hub y Azure no inicia la negociación si el extremo vecino utiliza el direccionamiento BGP APIPA. Es responsabilidad del dispositivo que se conecta a Azure iniciar la negociación BGP cuando se utiliza APIPA personalizado.

3) Compruebe la conectividad de capa 2.

```
show arp
```

4) Compruebe el routing de IP.

```
show route
```

5) Realice la captura en las interfaces ISP1 e ISP2.

```
capture isp1 interface ISP1 match udp any any eq 500
capture isp1 interface ISP1 match udp any any eq 4500
capture isp1 interface ISP1 match esp any any
...
show cap
show cap isp1
show cap isp2
```

6) Azure Verification: Vaya a vWAN Hub > Connectivity.> VPN Sites > Elija el sitio configurado.

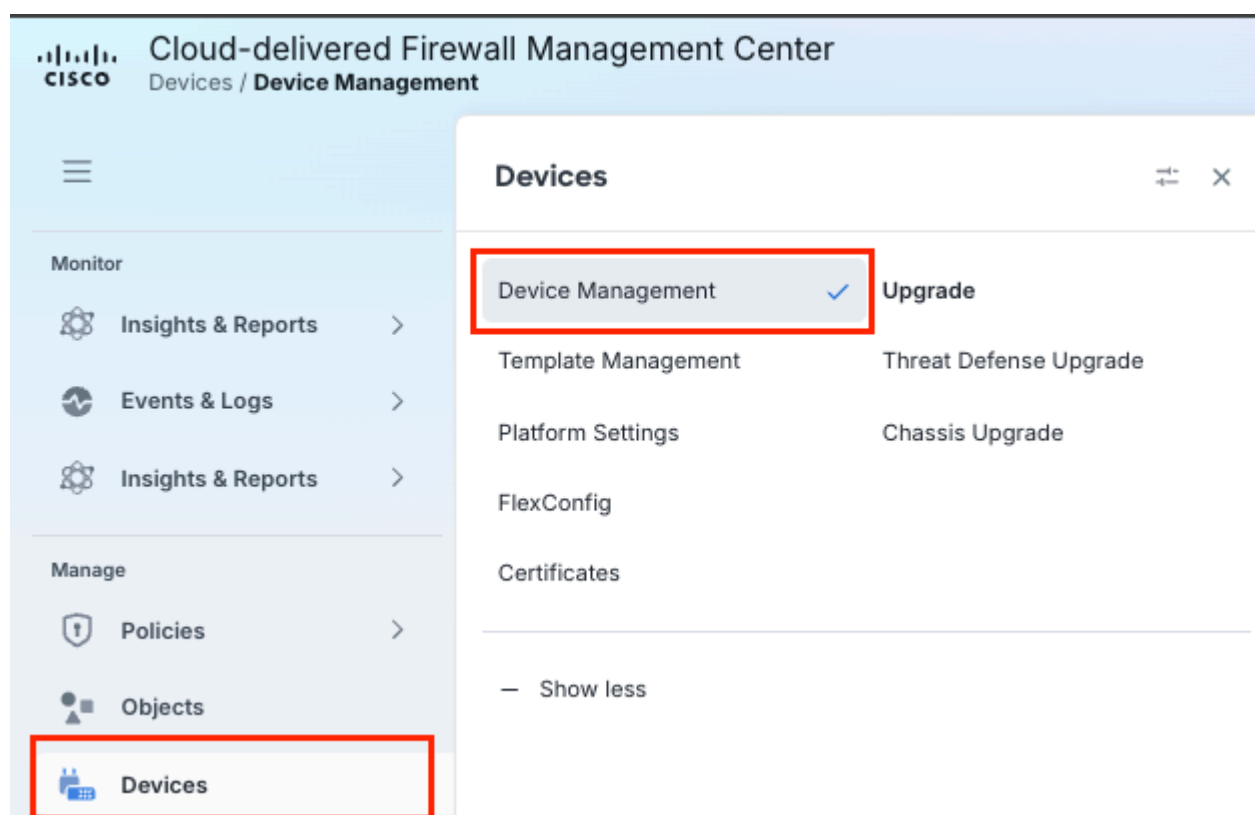
Links

☐ Link name	↑↓ Link provider name	↑↓ Connectivity status	↑↓ Hub name
☐ ISP-1-Link	ISP1	Instance0: Connected, Instance1: Connected	CX-vWAN-Hub
☐ ISP-2-Link	ISP2	Instance0: Connected, Instance1: Connected	CX-vWAN-Hub

Verificación de conectividad de Azure Link

Paso 7: Configuración de ECMP

1) Navegue hasta Manage > Devices > Device Management y haga clic en el FTD.



Vaya A Administración De Dispositivos En Firepower Management Center

N/A - ROUTED		
☐	☒ CXvWAN-FTD-2 N/A - ROUTED	10.0.0

Seleccione el FTD para la implementación de la configuración

2) Haga clic en la pestaña Routing y elija ECMP.

Device Interfaces Inline Sets **Routing** DHCP VTEP SNMP

Virtual Router Properties

These are the basic details of this virtual router.

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

VRF Name:

Global

Description:

This is a Global Virtual Router

Select Interface:

Search

Parámetros de configuración de múltiples rutas de igual coste

3) Haga clic en Agregar.

Equal-Cost Multipath Routing (ECMP)

Add

There are no ECMP zone records [Add](#)

Agregar opciones de configuración de múltiples rutas de igual costo

4) Asigne un nombre a la zona ECMP, haga clic en las interfaces VTI disponibles y, a continuación, haga clic en el botón Agregar para aplicarlas a la columna Interfaces seleccionadas y haga clic en Aceptar.

Add ECMP



Name

VTI-ECMP

Available Interfaces

ISP1

ISP2

Add

Selected Interfaces

ISP2-Inst-0



ISP2-Inst-1



ISP1-Inst-0



ISP1-Inst-1



Cancel

OK

Seleccione Interfaces Para La Zona De Trayectoria Múltiple De Igual Costo

5) Asegúrese de guardar los cambios.

You have unsaved changes

Save

Cancel

Guardar cambios

Paso 8: Configuración de BGP

1) Habilite el proceso BGP en el FTD bajo Routing > General Settings > BGP. Marque la casilla de verificación Enable BGP e ingrese el número AS configurado anteriormente en la Fase 1, Paso 1d. Vaya a Routing > BGP > IPv4.

Device

Interfaces

Inline Sets

Routing

DHCP

VTEP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

✓ BGP

IPv4

IPv6

Static Route

✓ Multicast Routing

IGMP

PIM

Multicast Routes

Multicast Boundary
Filter

General Settings

BGP

Enable BGP: ☒

AS Number*

65532

(1-4294967295 or 1.0-65535.65535)

☐ Override BGP general settings router-

Router Id

Automatic

IP Address*

General

Scanning Interval

Number of AS numbers in AS_PATH at

Log Neighbor Changes

Use TCP path MTU discovery

Reset session upon failover

Enforce the first AS is peer's AS for EB

Use dot notation for AS number

Aggregate Timer

BGP community new format (AA:NN)

Best Path Selection

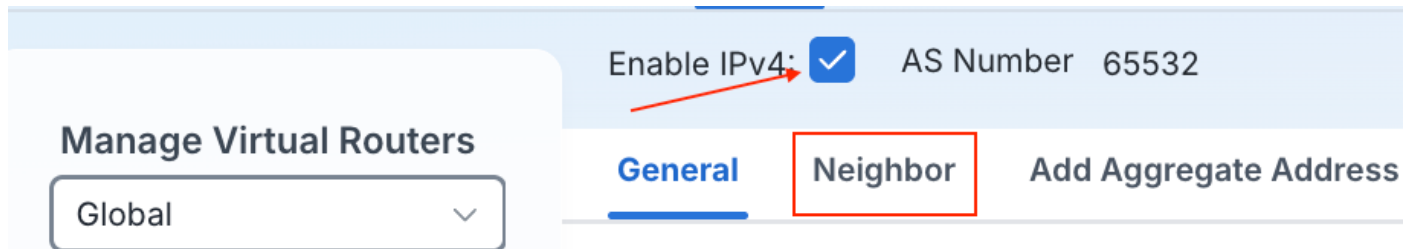
Default local preference

Allow comparing MED from different n

Compare Router ID for identical EBGP

Habilite el proceso de protocolo de gateway fronterizo en la configuración general

2) Asegúrese de marcar la casilla de verificación Enable IPv4 para el proceso BGP y haga clic en Neighbor para configurar los vecinos BGP en Azure.



Manage Virtual Routers

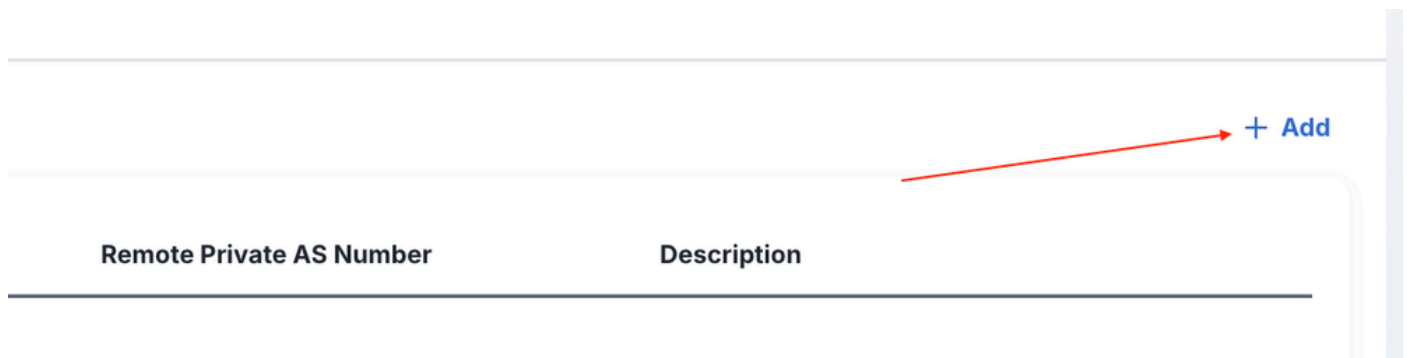
Global

Enable IPv4: ☒ AS Number 65532

General Neighbor Add Aggregate Address

Habilitar proceso de protocolo de gateway fronterizo IPv4

3) Haga clic en + Agregar.



+ Add

Remote Private AS Number	Description
--------------------------	-------------

Agregar nuevo vecino de protocolo de gateway fronterizo

4) Ingrese la información de peering BGP de Instancia0 ISP1, haga referencia al AS BGP notado del vWAN Hub e ingréselo como el AS remoto del vecino, y agregue una descripción si lo desea. Haga clic en Advanced.



Nota: Asegúrese de elegir BGP Update Source para hacer referencia al loopback para las interfaces VTI en el FTD asignado al link ISP1 configurado en Azure.

Add Neighbor ?

IP Address*

169.254.21.2

Remote AS*

65515

(1-4294967295 or 1.0-65535.65535)

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

BFD Fallover

none

Description

Update Source:

bgpLo-ISP1

Filtering Routes

Routes

Timers

Advanced

Migration

Configuración de Información de Peering de Border Gateway Protocol

5) Dentro del menú Advanced de la configuración BGP Neighbor en FTD, puede cambiar el número de saltos de Tiempo de Vida (TTL) del valor predeterminado de eBGP de 1 salto a un número variable. Los extremos BGP de Azure no están conectados directamente a través del túnel a la infraestructura de Azure y suele haber más saltos al extremo que los que permite el TTL de eBGP predeterminado de 1. Click OK.

Filtering Routes

Routes

Timers

Advanced

Migration

☐ Enable Authentication

Enable Encryption

0

Password

Confirm Password

☐ Send Community attribute to this neighbor

☐ Use itself as next hop for this neighbor

☐ Disable Connection Verification

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

10

(1-255)

☐ Use TCP path MTU discovery

TCP Transport Mode

Default

Weight

0

(0-65535)

BGP Version

Default

Cancel

OK

Configuración avanzada de vecino de protocolo de gateway fronterizo

6) Repita los pasos secundarios 3-5 para configurar Tunnel2 para ISP1 Instance1.

7) Repita los subpasos 3-5 dos veces para configurar la información de peering BGP de Instancia0/Instancia1 ISP2.



Nota: Asegúrese de elegir el Origen de actualización de BGP alineado que hace referencia al Loopback para las interfaces VTI en el FTD asignado al link ISP2 configurado en Azure.

Add Neighbor



IP Address*

169.254.21.22

Remote AS*

65515

(1-4294967295 or 1.0-65535.65535)

☒ Enabled address

☐ AS Override

☐ Shutdown administratively

☐ Configure graceful restart (failover/spanned mode)

☐ Enable graceful restart

BFD Fallover

none

Description

Update Source:

bgpLo-ISP2

Filtering Routes

Routes

Timers

Advanced

Migration

☐ Enable Authentication

Enable Encryption

0

Password

Confirm Password

☐ Send Community attribute to this neighbor

☐ Use itself as next hop for this neighbor

☐ Disable Connection Verification

☒ Allow connections with neighbor that is not directly connected

☐ Limited number of TTL hops to neighbor

TTL Hops

10

(1-255)

☐ Use TCP path MTU discovery

TCP Transport Mode

Cancel

OK

Configuración del Vecino BGP de Instancia 1 ISP2

Add Neighbor



IP Address*

169.254.22.22

Remote AS*

65515

(1-4294967295 or 1.0-65535.65535)

- ☒ Enabled address
- ☐ AS Override
- ☐ Shutdown administratively
- ☐ Configure graceful restart (failover/spanned mode)
- ☐ Enable graceful restart

BFD Fallover

none

Description

Update Source:

bgpLo-ISP2

Filtering Routes Routes Timers **Advanced** Migration

- ☐ Enable Authentication
- Enable Encryption
- 0
- Password
-
- Confirm Password
-
- ☐ Send Community attribute to this neighbor
- ☐ Use itself as next hop for this neighbor
- ☐ Disable Connection Verification
- ☒ Allow connections with neighbor that is not directly connected
- ☐ Limited number of TTL hops to neighbor
- TTL Hops
- 10
- (1-255)
- ☐ Use TCP path MTU discovery
- TCP Transport Mode
-

Cancel

OK

Configuración de Vecino BGP de Instancia 2 de ISP

Address	Remote AS Number	Address Family	Remote Private AS Number	Description
169.254.21.2	65515	Enabled		
169.254.22.2	65515	Enabled		
169.254.21.22	65515	Enabled		
169.254.22.22	65515	Enabled		

Finalizar configuración de resultado de vecino BGP

Una vez finalizado, haga clic en Guardar.

You have unsaved changes

Save

Guardar cambios

De forma predeterminada, BGP instala solamente una única mejor trayectoria en la tabla de ruteo, aunque ECMP esté configurado en todas las VTI a Azure. Las múltiples trayectorias BGP deben habilitarse por separado para que ambas trayectorias aprendidas se instalen y utilicen al mismo tiempo.

Paso 9: Configuración de Trayectoria Múltiple eBGP

1) Navegue hasta Routing > BGP > IPv4, haga clic en la pestaña General y haga clic en el icono de lápiz adyacente a Forward Packets Over Multiple Paths.

Enable IPv4: ☒ AS Number 65532

Manage Virtual Routers

Global

Virtual Router Properties

- ECMP
- BFD
- OSPF
- OSPFv3
- EIGRP
- RIP
- Policy Based Routing
- BGP**
- IPv4
- IPv6
- Static Route
- Multicast Routing
 - IGMP
 - PIM
 - Multicast Routes
 - Multicast Boundary Filter

General Settings

BGP

General Neighbor Add Aggregate Address Filtering Networks Redistribution Ro

Setting

Learned Route Map

Administrative Route Distances

External	20
Internal	200
Local	200

Routes and Synchronization

Generate default routes	No
Summarize subnet routes into network level routes	No
Advertise inactive routes	Yes
Synchronize between BGP and IGP systems	No
Redistribute IBGP into IGP	No
(Use filtering to limit the number of prefixes that are redistributed)	

Forward Packets Over Multiple Paths

Number of Paths	1
IBGP number of paths	1

Configuración de reenvío de paquetes a través de varias rutas

2) Cambie el valor predeterminado del campo Número de rutas de 1 a 4. Haga clic en Aceptar.

Edit Forward packets Over Multiple Paths ?

Number of Paths

4

IBGP Number of Paths

1

Cancel

OK

Cambiar la configuración de reenvío de paquetes en varias rutas

3) Asegúrese de guardar e implementar los cambios.

Verificar/Solucionar problemas

Una vez completada la implementación, confirme que el proceso BGP de FTD establece adyacencias de vecinos con ambas instancias de Azure en los túneles respectivos y que se aprenden las rutas, las interfaces están activas y las conexiones de protocolo se devuelven en la tabla de conexiones.

Navegue hasta `system support diagnostic-cli` en la CLI de FTD como se hizo en la Fase 2, Paso 7.

1) Una vez implementado, se espera que los vecinos BGP aparezcan y se reciban los prefijos.

```
<#root>
```

```
>
```

```
system support diagnostic-cli
```

```
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
```

```
Type help or '?' for a list of available commands.
```

```
ftd#
```

```
ftd#
```

```
ftd#
```

```
show bgp summary
```

```
BGP router identifier 169.254.22.100, local AS number 65532
```

```

BGP table version is 29, main routing table version 29
2 network entries using 400 bytes of memory
8 path entries using 640 bytes of memory
2 multipath network entries and 8 multipath paths
1/1 BGP path/bestpath attribute entries using 208 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1272 total bytes of memory
BGP activity 4/2 prefixes, 16/8 paths, scan interval 60 secs

```

```

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
169.254.21.2 4 65515 20 17 29 0 0 00:13:14 2
169.254.22.2 4 65515 20 20 29 0 0 00:13:22 2
169.254.21.22 4 65515 19 21 29 0 0 00:13:19 2
169.254.22.22 4 65515 20 19 29 0 0 00:13:17 2
ftd#

```

2) Compruebe que las rutas recibidas de Azure se muestren como rutas de múltiples rutas.

```
<#root>
```

```
ftd#
```

```
show bgp
```

```

BGP table version is 29, local router ID is 169.254.22.100
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath
Origin codes: i - IGP, e - EGP, ? - incomplete

```

Network	Next Hop	Metric	LocPrf	Weight	Path
*m 10.2.0.0/16	169.254.21.2			0	65515 i
*m	169.254.22.22			0	65515 i
*m	169.254.21.22			0	65515 i
*>	169.254.22.2			0	65515 i
*m 172.27.0.0	169.254.21.2			0	65515 i
*m	169.254.22.22			0	65515 i
*m	169.254.21.22			0	65515 i
*>	169.254.22.2			0	65515 i

3) Verifique el relleno de la tabla de ruteo.

```
<#root>
```

```
ftd#
```

```
show route bgp
```

```

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN

```

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route, + - replicated route
 SI - Static InterVRF, BI - BGP InterVRF

Gateway of last resort is 172.31.3.33 to network 0.0.0.0

```
B      10.2.0.0 255.255.0.0 [20/0] via 169.254.22.22, 00:20:53
      [20/0] via 169.254.22.2, 00:20:53
      [20/0] via 169.254.21.22, 00:20:53
      [20/0] via 169.254.21.2, 00:20:53
B      172.27.0.0 255.255.0.0 [20/0] via 169.254.22.22, 00:20:53
      [20/0] via 169.254.22.2, 00:20:53
      [20/0] via 169.254.21.22, 00:20:53
      [20/0] via 169.254.21.2, 00:20:53
```

4) Verifique la tabla de conexión para las sesiones BGP.

<#root>

ftd#

show conn all | include TCP|179

```
TCP ISP2-Inst-0 169.254.21.22:179 bgpLo-ISP2 169.254.22.100:1603, idle 0:00:10, bytes 1517, flags UIO
TCP ISP2-Inst-1 169.254.22.22:179 bgpLo-ISP2 169.254.22.100:41883, idle 0:00:01, bytes 1486, flags UIO
TCP ISP1-Inst-1 169.254.22.2:179 bgpLo-ISP1 169.254.21.100:3804, idle 0:00:53, bytes 1467, flags UIO
TCP ISP1-Inst-0 169.254.21.2:179 bgpLo-ISP1 169.254.21.100:61287, idle 0:00:04, bytes 1331, flags UIO
TCP bgpLo-ISP1 169.254.22.2:179 NP Identity Ifc 169.254.21.100:3804, idle 0:00:53, bytes 751, flags U
TCP bgpLo-ISP2 169.254.21.22:179 NP Identity Ifc 169.254.22.100:1603, idle 0:00:10, bytes 844, flags U
TCP bgpLo-ISP2 169.254.22.22:179 NP Identity Ifc 169.254.22.100:41883, idle 0:00:01, bytes 751, flags U
TCP bgpLo-ISP1 169.254.21.2:179 NP Identity Ifc 169.254.21.100:61287, idle 0:00:04, bytes 639, flags U
```

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).